PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-344925
(43)Date of publication of application : 14.12.1999

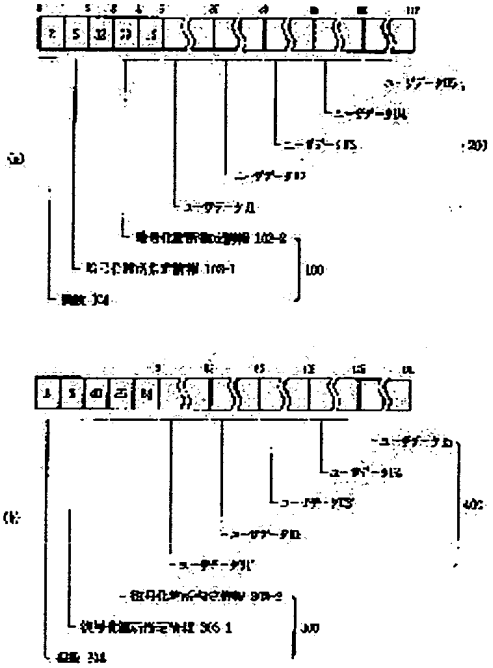
(51)Int.Cl. G09C 1/00
H04L 9/14
H04L 9/34

(21)Application number : 10-166004
(22)Date of filing : 29.05.1998

(71)Applicant : NEC CORP
(72)Inventor : KITAMOTO YOHEI

(54) PARTIAL CIPHERING DEVICE AND RECORDING MEDIUM READABLE BY COMPUTER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a partial ciphering device capable of more finely specifying a point to be ciphered in a series of data.
SOLUTION: An information frame having a data part 200 and a ciphering control information part 100 including one or more pieces of ciphering point specification information 103-1, 103-2, in which a starting position of the data to be ciphered among a series of the data stored in the data part 200 and its length are specified and its number 104 is inputted by the partial ciphering device. And an information frame having a data part 400 in which only the data at the point specified by the ciphering control information part 100 among a series of the data is ciphered and a decoding control information part 300 in which the number of pieces of the data to be decoded, its starting position and length are specified among a series of the data stored in the data part 400 is generated and outputted.



LEGAL STATUS

[Date of request for examination] 29.05.1998
[Date of sending the examiner's decision of rejection] 13.11.2001
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－344925

(43)公開日　平成11年(1999)12月14日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０９Ｃ	1/00	６１０	Ｇ０９Ｃ	1/00	６１０Ｚ
Ｈ０４Ｌ	9/14		Ｈ０４Ｌ	9/00	６４１
	9/34				６８１

審査請求　有　　請求項の数７　ＦＤ　（全 13 頁）

(21)出願番号　特願平10－166004

(22)出願日　平成10年(1998)５月29日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　北本　洋平
東京都港区芝五丁目７番１号　日本電気株式会社内

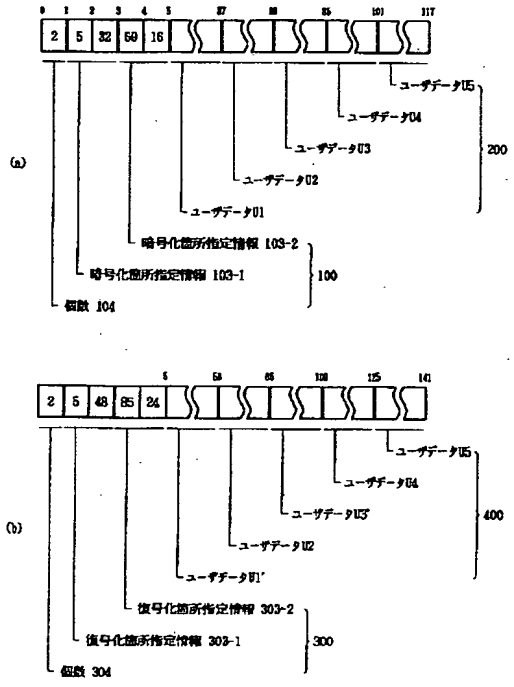
(74)代理人　弁理士　境　廣巳

(54)【発明の名称】　部分的暗号化装置及びコンピュータ可読記録媒体

(57)【要約】

【課題】　一連のデータ中の暗号化したい箇所をよりきめ細かく指定することができる部分的暗号化装置を提供する。

【解決手段】　部分的暗号化装置は、データ部200 とこのデータ部200 に格納された一連のデータのうち暗号化対象となるデータの開始位置及びその長さを指定した１つ以上の暗号化箇所指定情報103-1, 103-2 とその個数104 とを含む暗号化制御情報部100 とを有する情報フレームを入力し、一連のデータのうち暗号化制御情報部100 で指定された箇所のデータのみを暗号化したデータ部400 と、このデータ部400 に格納された一連のデータのうち復号化対象となるデータの個数とその開始位置及び長さを指定した復号化制御情報部300 とを有する情報フレームを生成し、出力する。



1

【特許請求の範囲】

【請求項１】　データ部と該データ部に格納された一連のデータのうち暗号化対象となるデータの開始位置及びその長さを指定した暗号化制御情報部とを有する情報フレームを入力する入力手段と、前記一連のデータのうち前記暗号化制御情報部で指定された箇所のデータのみを暗号化したデータ部と該データ部に格納された一連のデータのうち復号化対象となるデータの開始位置及びその長さを指定した復号化制御情報部とを有する情報フレームを生成する暗号化制御手段と、前記生成された情報フレームを出力する出力手段とを備えることを特徴とする部分的暗号化装置。

【請求項２】　前記入力手段で入力される情報フレームの暗号化制御情報部が、暗号化対象となるデータの開始位置及びその長さを指定した１つの暗号化箇所指定情報を含むことを特徴とする請求項１記載の部分的暗号化装置。

【請求項３】　前記入力手段で入力される情報フレームの暗号化制御情報部が、暗号化対象となるデータの開始位置及びその長さを指定した１つ以上の暗号化箇所指定情報と該暗号化箇所指定情報の個数とを含むことを特徴とする請求項１記載の部分的暗号化装置。

【請求項４】　暗号化対象となるデータを同じサイズのデータに暗号化する暗号手段を備えることを特徴とする請求項２または３記載の部分的暗号化装置。

【請求項５】　暗号化対象となるデータをそれよりサイズの大きなデータに暗号化する暗号手段を備えることを特徴とする請求項２または３記載の部分的暗号化装置。

【請求項６】　前記入力手段は、情報処理装置上で稼働する複数の業務プログラムのうちの任意の業務プログラムから情報フレームを入力する構成を有することを特徴とする請求項４または５記載の部分的暗号化装置。

【請求項７】　情報処理装置を、データ部と該データ部に格納された一連のデータのうち暗号化対象となるデータの開始位置及びその長さを指定した暗号化制御情報部とを有する情報フレームを入力する入力手段、前記一連のデータのうち前記暗号化制御情報部で指定された箇所のデータのみを暗号化したデータ部と該データ部に格納された一連のデータのうち復号化対象となるデータの開始位置及びその長さを指定した復号化制御情報部とを有する情報フレームを生成する暗号化制御手段、前記生成された情報フレームを出力する出力手段、として機能させるプログラムを記録したコンピュータ可読記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は暗号化装置に関し、より詳細には、一連のデータのうちの指定された箇所のみ暗号化する機能を有する部分的暗号化装置に関する。

【０００２】

【従来の技術】データの暗号化は、例えば通信回線でつながれた情報処理装置間でデータを送受信する場合などに機密の漏洩を防止するために実施されている。データの暗号方式には、使用する鍵の種類によって、共通鍵を使用する共通鍵方式と公開鍵を使用する公開鍵方式とに大別され、また、暗号化前後のデータサイズによって、暗号化前後で同一サイズとなる暗号方式と、暗号化によってデータサイズが拡大する暗号方式とに大別される。何れの方式でも暗号化対象となるデータ長が長くなればなるほど、暗号化処理により多くの時間がかかることにかわりはない。

2

【０００３】そこで、同時に送信する複数のデータ間に重要度の差異がある場合、重要度の高いデータのみ暗号化し、それ以外のデータはそのまま送信することにより、暗号化処理時間を短縮することが考えられる。例えば、情報処理装置上に２つの業務プログラムＡ，Ｂがあり、業務プログラムＡは図２０（ａ）に示すように１回の送信でａ１，ａ２，ａ３という３種類のデータを含む一連のデータを送信し、業務プログラムＢは図２０（ｂ）に示すように１回の送信でｂ１，ｂ２という２種類のデータを含む一連のデータを送信し、データａ２とデータｂ２とが機密情報であるとする。この場合、業務プログラムＡは、データａ１，ａ２，ａ３からなる一連データを生成後、データａ２のみを暗号化し、得られた暗号データａ２’と残りのデータａ１，ａ３とで一連データを再作成して相手装置に送信する。業務プログラムＢも同様に、データｂ１，ｂ２からなる一連データを生成後、データｂ２のみを暗号化し、得られた暗号データｂ２’と残りのデータｂ１とで一連データを再作成して相手装置に送信する。こうすることにより、データ全体（ａ１～ａ３，ｂ１～ｂ２）を暗号化するのに比べて、暗号化処理に要する時間が短縮できる。

【０００４】しかしながら、以上のような部分的な暗号化処理を各業務プログラムが実施する構成では、各業務プログラムの負荷が大きくなり過ぎる。このような問題を解決するには、一連のデータのうちの指定された箇所を暗号化する機能を有する部分的暗号化装置が必要である。

【０００５】このような部分的暗号化装置に応用可能な従来技術が特開平２－１８８７８２号公報に開示されている。同公報に記載された暗号化装置は、パラメータとして、メッセージ格納域アドレス，メッセージ長，暗号処理を開始するメッセージ上の位置等を受け取って暗号化処理を実施する。暗号処理を開始するメッセージ上の位置は通常通信メッセージの開始位置が指定されており、暗号化装置は、このパラメータの指定に従い、通信ヘッダ部は暗号化せず、通信メッセージ部のみを暗号化する。

【０００６】

【発明が解決しようとする課題】上述した従来の暗号化装置を応用すれば、前述した業務プログラムＢの場合、

図２０（ｂ）に示したデータｂ１，データｂ２からなる一連データの生成後、データｂ２の先頭を開始位置に指定して暗号化装置に通知することにより、データｂ２のみを暗号化した一連データを得ることができる。しかしながら、前述した業務プログラムＡの場合、図２０（ａ）に示したように暗号化したいデータａ２は中間に位置するので、データａ２の先頭を開始位置に指定して暗号化装置に通知すると、データａ２だけでなく、後続のデータａ３も暗号化されてしまうという問題がある。

【０００７】そこで本発明の目的は、一連のデータ中の暗号化したい箇所をよりきめ細かく指定することができる部分的暗号化装置を提供することにある。

【０００８】

【課題を解決するための手段】本発明の部分的暗号化装置は、データ部と該データ部に格納された一連のデータのうち暗号化対象となるデータの開始位置及びその長さを指定した暗号化制御情報部とを有する情報フレームを入力する入力手段と、前記一連のデータのうち前記暗号化制御情報部で指定された箇所のデータのみを暗号化したデータ部と該データ部に格納された一連のデータのうち復号化対象となるデータの開始位置及びその長さを指定した復号化制御情報部とを有する情報フレームを生成する暗号化制御手段と、前記生成された情報フレームを出力する出力手段とを備える。

【０００９】前記入力手段で入力される情報フレームの暗号化制御情報部は、暗号化対象となるデータの開始位置及びその長さを指定した１つの暗号化箇所指定情報を含んだ構成でも良く、暗号化対象となるデータの開始位置及びその長さを指定した１つ以上の暗号化箇所指定情報と該暗号化箇所指定情報の個数とを含んだ構成でも良い。また、暗号化対象となるデータを暗号化する手段は任意であり、共通鍵方式や公開鍵方式、同じサイズのデータに暗号化する暗号方式や、よりサイズの大きなデータに暗号化する暗号方式が採用できる。さらに、入力手段は、情報処理装置上で稼働する複数の業務プログラムのうちの任意の業務プログラムから情報フレームを入力することで、本発明の部分的暗号化装置が複数の業務プログラムで共通に使用できるようになっている。

【００１０】

【発明の実施の形態】次に本発明の実施の形態の例について図面を参照して詳細に説明する。

【００１１】図１は本発明を適用した情報処理装置の一例を示すブロック図である。この例の情報処理装置１は、通信回線２を介して他の情報処理装置（図示せず）と接続されており、複数の業務プログラム３－１～３－ｍと、データ送受信装置４と、本発明にかかる部分的暗号化装置５および部分的復号化装置６とを有している。また、７はＣＤ－ＲＯＭ，磁気ディスク，半導体メモリ等の機械読み取り可能な記録媒体であり、ここに記録されたプログラムは情報処理装置１によって読み取られ、

情報処理装置１の動作を制御することにより、情報処理装置１上に部分的暗号化装置５および部分的復号化装置６を実現する。

【００１２】各々の業務プログラム３－１～３－ｍは、他の情報処理装置に対して一連のデータを送信する場合、それらのデータを格納したデータ部と、このデータ部に格納された一連のデータのうち暗号化対象となるデータの開始位置及びその長さを指定した暗号化制御情報部とを有する情報フレームを、送り先の情報および送り元の情報と共に部分的暗号化装置５に送出する。部分的暗号化装置５は、業務プログラム３－１～３－ｍから入力した情報フレームの暗号化制御情報部を解析し、データ部中の暗号化すべき箇所のみを暗号化したデータ部と、このデータ部に格納された一連のデータのうち復号化対象となるデータの開始位置及びその長さを指定した復号化制御情報部とを有する情報フレームを生成し、送り先の情報および送り元の情報と共にデータ送受信装置４に送出する。データ送受信装置４は、入力した情報フレームに送り元の情報等を付加して、送り先の他情報処理装置に通信回線２を介して送信する。

【００１３】他方、他の情報処理装置で同様にして作成されて通信回線２を介して送られてきた情報フレームをデータ送受信装置４が受信すると、送り先の情報および送り元の情報と共にその情報フレームが部分的復号化装置６に送出される。部分的復号化装置６は、データ送受信装置４から入力した情報フレームの復号化制御情報部を解析し、データ部中の復号化すべき箇所のみを復号化したデータ部と、このデータ部に格納された一連のデータのうち暗号化対象となるデータの開始位置及びその長さを指定した暗号化制御情報部とを有する情報フレームを生成し、送り元の情報と共に、送り先の業務プログラム３－１～３－ｍに送出する。なお、暗号化制御情報部は省略しても良い。

【００１４】図２は部分的暗号化装置５の構成例を示すブロック図である。この例の部分的暗号化装置５は、入力手段５１と、暗号化制御手段５２と、暗号手段５３と、出力手段５４とから構成されている。入力手段５１は、任意の業務プログラム３－１～３－ｍから情報フレームを入力すると、それを暗号化制御手段５２に渡す。暗号化制御手段５２は、情報フレームの暗号化制御情報部を解析し、データ部に格納されている一連のデータのうち暗号化制御情報部で指定された箇所のデータのみを暗号手段５３で暗号化し、それ以外の部分は元のままのデータとしたデータ部と、このデータ部に格納された一連のデータのうち復号化対象となるデータの開始位置及びその長さを指定した復号化制御情報部とを有する情報フレームを生成する。出力手段５４は、暗号化制御手段５２で生成された情報フレームを、業務プログラム３－１～３－ｍから情報フレームの入力時に入力された送り先および送り元の情報を添えて、データ送受信装置４に

送出する。

【００１５】図３は部分的復号化装置６の構成例を示すブロック図である。この例の部分的復号化装置６は、入力手段６１と、復号化制御手段６２と、復号手段６３と、出力手段６４とから構成されている。入力手段６１は、データ送受信装置４から情報フレームを入力すると、それを復号化制御手段６２に渡す。復号化制御手段６２は、情報フレームの復号化制御情報部を解析し、データ部に格納されている一連のデータのうち復号化制御情報部で指定された箇所のデータのみを復号手段６３で復号化し、それ以外の部分は元のままのデータとしたデータ部と、このデータ部に格納された一連のデータのうち暗号化対象となるデータの開始位置及びその長さを指定した暗号化制御情報部とを有する情報フレームを生成する。出力手段６４は、復号化制御手段６２で生成された情報フレームを、データ送受信装置４から情報フレームの入力時に入力された送り元の情報を添えて、送り先の業務プログラム３－１～３－ｍに送出する。

【００１６】

【実施例】次に本発明の実施例について図面を参照して詳細に説明する。実施例としては、以下のものを取り上げる。

（１）暗号化する箇所を複数指定可能な実施例

（２）暗号化する箇所を１つのみ指定可能な実施例

また、その各々について、暗号化によりデータサイズが拡大する場合と拡大しない場合（つまり同一サイズになる場合）とについて説明する。

【００１７】（１）暗号化する箇所を複数指定可能な実施例

図４（ａ）は業務プログラム３－１～３－ｍから部分的暗号化装置５に入力される情報フレームのフォーマット例を示す図である。この例の情報フレームは、暗号化制御情報部１００と、複数のユーザデータから構成されるデータ部２００とから構成されている。暗号化制御情報部１００は、図４（ｂ）に示すように、データ部２００に格納された一連のユーザデータのうち暗号化対象となるデータの開始位置１０１及びそのバイト数１０２を指定した１つ以上の暗号化箇所指定情報１０３と、この暗号化箇所指定情報１０３の個数１０４とを含む。開始位置１０１，バイト数１０２および個数１０４のサイズは固定長である。図４（ｃ）に、開始位置１０１及びバイト数１０２とユーザデータとの関連、個数１０４と暗号化箇所指定情報１０３との関連を示す。開始位置１０１としては、例えば情報フレームの先頭の１バイト（つまり個数１４０の先頭バイト）目を０バイト目とした場合の、当該ユーザデータの先頭バイトまでのバイト数で表現される。なお、本実施例では、部分的復号化装置６から業務プログラム３－１～３－ｍに入力される情報フレームも図４（ａ）の形式としている。

【００１８】他方、図４（ｄ）は部分的暗号化装置５からデータ送受信装置４に入力される情報フレームのフォーマット例を示す図である。この例の情報フレームは、復号化制御情報部３００と、複数のユーザデータから構成されるデータ部４００とから構成されている。復号化制御情報部３００は、図４（ｅ）に示すように、データ部４００に格納された一連のユーザデータのうち復号化対象となるデータの開始位置３０１及びそのバイト数３０２を指定した１つ以上の復号化箇所指定情報３０３と、この復号化箇所指定情報３０３の個数３０４とを含む。開始位置３０１，バイト数３０２および個数３０４のサイズは固定長である。開始位置３０１としては、例えば情報フレームの先頭の１バイト（つまり個数３０４の先頭バイト）目を０バイト目とした場合の、当該ユーザデータまでのバイト数で表現される。なお、本実施例では、データ送受信装置４から部分的復号化装置６に入力される情報フレームも図４（ｄ）の形式としている。

【００１９】（Ａ）暗号化によりデータサイズが拡大する場合

【００２０】（ア）暗号化

この場合の部分的暗号化装置５の処理の一例を図５のフローチャートに示す。何れかの業務プログラム３－１～３－ｍから図４（ａ）に示したような形式の情報フレームが送られると、入力手段５１がそれを入力し（ステップＳ１）、暗号化制御手段５２に伝達する。暗号化制御手段５２は、情報フレームの暗号化制御情報部１００を解析し（ステップＳ２）、解析結果を制御テーブルに設定する（ステップＳ３）。

【００２１】例えば、図６に示すように、各々３２バイト，３２バイト，１６バイト，１６バイト，１６バイトである５つのユーザデータＵ１，Ｕ２，Ｕ３，Ｕ４，Ｕ５を含むデータ部２００と、ユーザデータＵ１，Ｕ３を暗号化対象として指定した２つの暗号化箇所指定情報１０３－１，１０３－２と個数「２」とを含む暗号化制御情報部１００とから構成される情報フレームの場合、個数，開始位置，バイト数のサイズを例えば１バイト固定とすると、情報フレームの先頭から５～３７バイト目のユーザデータＵ１と６９～８５バイト目のユーザデータＵ３とが暗号化対象データであり、ユーザデータＵ１とユーザデータＵ３との間のユーザデータＵ２、ユーザデータＵ３より後ろのデータ（ユーザデータＵ４，Ｕ５）は暗号化対象データでないので、例えば図７に示すような４つのエントリＥ１，Ｅ２，Ｅ３，Ｅ４を持つ制御テーブル９００を生成し、開始位置，バイト数，暗号化の有無の欄にそれぞれ図示する値を設定する。なお、この時点では、暗号化後の開始位置，暗号化後のバイト数の欄はＮＵＬＬである。

【００２２】次に暗号化制御手段５２は、制御テーブル９００の暗号化の有無の欄が「有」になっているエントリＥ１，Ｅ３毎に、該当する箇所のデータをデータ部２００から取り出し、暗号手段５３に与えることにより暗

号化する（ステップＳ４）。

【００２３】次に暗号化制御手段５２は、暗号化後のデータサイズを図７に示すように、エントリＥ１，Ｅ３の暗号化後のバイト数の欄に設定し、それに基づいて暗号化後の開始位置の欄に値を設定する（ステップＳ５）。例えば、エントリＥ１の暗号化後のバイト数は「４８」に拡大したので、エントリＥ２の暗号化後の開始位置は「５３」に設定される。

【００２４】次に暗号化制御手段５２は、図７の制御テーブル９００の暗号化の有無の欄が「有」になっているエントリＥ１，Ｅ３の個数「２」を個数３０４、エントリＥ１の暗号化後の開始位置「５」と暗号化後のバイト数「４８」との組、エントリＥ３の暗号化後の開始位置「８５」と暗号化後のバイト数「２４」との組をそれぞれ復号化箇所指定情報３０３－１，３０３－２とした復号化制御情報部３００を生成する（ステップＳ６）。これにより、図６（ｂ）に示す復号化制御情報部３００が生成される。

【００２５】次に暗号化制御手段５２は、図７の制御テーブル９００のエントリＥ１から順にエントリＥ４まで、そのエントリの暗号化の有無の欄が「有」であれば暗号化後のデータを、「無」であれば、制御テーブル９００の開始位置の欄とバイト数の欄とで特定される入力情報フレーム上の元のデータを、データ部の先頭から順に詰め込んで、データ部４００を生成する（ステップＳ７）。これにより、図６（ｂ）に示すデータ部４００が生成される。

【００２６】以上のようにして復号化制御情報部３００とデータ部４００とから構成される情報フレームが生成されると、出力手段５４が、送り先および送り元の情報と共に情報フレームをデータ送受信装置４に送る（ステップＳ８）。

【００２７】（イ）復号化

この場合の部分的復号化装置６の処理の一例を図８のフローチャートに示す。データ送受信装置４から図４（ｄ）に示したような形式の情報フレームが送られると、入力手段６１がそれを入力し（ステップＳ１１）、復号化制御手段６２に伝達する。復号化制御手段６２は、情報フレームの復号化制御情報部３００を解析し（ステップＳ１２）、解析結果を制御テーブルに設定する（ステップＳ１３）。

【００２８】例えば、入力された情報フレームが図６（ｂ）に示した情報フレームであった場合、情報フレームの先頭から５～５３バイト目のユーザデータＵ１’と８５～１０９バイト目のユーザデータＵ３’とが復号化対象データであり、ユーザデータＵ１’とユーザデータＵ３’との間のユーザデータＵ２、ユーザデータＵ３’より後ろのデータ（ユーザデータＵ４，Ｕ５）は復号化対象データでないので、例えば図９に示すような４つのエントリＥ１，Ｅ２，Ｅ３，Ｅ４を持つ制御テーブル９

０１を生成し、開始位置，バイト数，復号化の有無の欄にそれぞれ図示する値を設定する。なお、この時点では、復号化後の開始位置，復号化後のバイト数の欄はＮＵＬＬである。

【００２９】次に復号化制御手段６２は、制御テーブル９０１の復号化の有無の欄が「有」になっているエントリＥ１，Ｅ３毎に、該当する箇所のデータをデータ部４００から取り出し、復号手段６３に与えることにより復号化する（ステップＳ１４）。

【００３０】次に復号化制御手段６２は、復号化後のデータサイズを図９に示すように、エントリＥ１，Ｅ３の復号化後のバイト数の欄に設定し、それに基づいて復号化後の開始位置の欄に値を設定する（ステップＳ１５）。例えば、エントリＥ１の復号化後のバイト数は「３２」なので、エントリＥ２の復号化後の開始位置は「３７」に設定される。

【００３１】次に復号化制御手段６２は、図９の制御テーブル９０１の復号化の有無の欄が「有」になっているエントリＥ１，Ｅ３の個数「２」を個数１０４、エントリＥ１の復号化後の開始位置「５」と復号化後のバイト数「３２」との組、エントリＥ３の復号化後の開始位置「６９」と復号化後のバイト数「１６」との組をそれぞれ暗号化箇所指定情報１０３－１，１０３－２とした暗号化制御情報部１００を生成する（ステップＳ１６）。これにより、図６（ａ）に示す暗号化制御情報部１００が生成される。

【００３２】次に復号化制御手段６２は、図９の制御テーブル９０１のエントリＥ１から順にエントリＥ４まで、そのエントリの復号化の有無の欄が「有」であれば復号化後のデータを、「無」であれば、制御テーブル９０１の開始位置の欄とバイト数の欄とで特定される入力情報フレーム上の元のデータを、データ部の先頭から順に詰め込んで、データ部２００を生成する（ステップＳ１７）。これにより、図６（ａ）に示すデータ部２００が生成される。

【００３３】以上のようにして暗号化制御情報部１００とデータ部２００とから構成される情報フレームが生成されると、出力手段６４が、送り元の情報と共に送り先の業務プログラムに送る（ステップＳ１８）。

【００３４】（Ｂ）暗号化によりデータサイズが拡大しない場合

【００３５】（ア）暗号化

この場合の部分的暗号化装置５の処理の一例を図１０のフローチャートに示す。何れかの業務プログラム３－１～３－ｍから図４（ａ）に示したような形式の情報フレームが送られると、入力手段５１がそれを入力し（ステップＳ２１）、暗号化制御手段５２に伝達する。暗号化制御手段５２は、情報フレームの暗号化制御情報部１００を解析し、個数１０４を変数Ｍａｘに、初期値１を変数ｉに設定する（ステップＳ２２）。例えば図６（ａ）

に示した情報フレームの場合、Ｍａｘは２に設定される。

【００３６】次に暗号化制御手段５２は、暗号化制御情報部１００における先頭から変数ｉの値番目の暗号化箇所指定情報が示す箇所のデータを、データ部２００から取り出し（ステップＳ２３）、暗号手段５３に与えることにより暗号化する（ステップＳ２４）。そして、生成された暗号データで、データ部２００の元の箇所を上書きする（ステップＳ２５）。

【００３７】これで、１つの暗号化対象データについての処理を終えたことになり、変数ｉを＋１し（ステップＳ２６）、Ｍａｘ以下ならばステップＳ２３に戻って上述した処理を繰り返す。変数ｉがＭａｘより大きければ、全ての暗号化対象データの処理を終えたので、データ部が上書きされた情報フレームを、出力手段５４により、送り先および送り元の情報と共にデータ送受信装置４に送出する（Ｓ２８）。

【００３８】このように暗号化によってデータサイズが拡大せず同一サイズとなる場合、入力された情報フレームの暗号化制御情報部１００の内容は実質的に変更されず、そのまま復号化制御情報部３００となる。

【００３９】（イ）復号化

この場合の部分的復号化装置６の処理の一例を図１１のフローチャートに示す。データ送受信装置４から図４（ｄ）に示したような形式の情報フレームが送られると、入力手段６１がそれを入力し（ステップＳ３１）、復号化制御手段６２に伝達する。復号化制御手段６２は、情報フレームの復号化制御情報部３００を解析し、個数３０４を変数Ｍａｘに、初期値１を変数ｉに設定する（ステップＳ３２）。例えば図６（ｂ）に示した情報フレームの場合、Ｍａｘは２に設定される。

【００４０】次に復号化制御手段６２は、復号化制御情報部３００における先頭から変数ｉの値番目の復号化箇所指定情報が示す箇所のデータを、データ部４００から取り出し（ステップＳ３３）、復号手段６３に与えることにより復号化する（ステップＳ３４）。そして、生成された復号データで、データ部４００の元の箇所を上書きする（ステップＳ３５）。

【００４１】これで、１つの復号化対象データについての処理を終えたことになり、変数ｉを＋１し（ステップＳ３６）、Ｍａｘ以下ならばステップＳ３３に戻って上述した処理を繰り返す。変数ｉがＭａｘより大きければ、全ての復号化対象データの処理を終えたので、データ部が上書きされた情報フレームを、出力手段６４により、送り元の情報と共に送り先の業務プログラムに送出する（Ｓ３８）。

【００４２】このように復号化によってデータが拡大せず同一サイズとなる場合、入力された情報フレームの復号化制御情報部３００の内容は実質的に変更されず、そのまま暗号化制御情報部１００となる。

【００４３】（２）暗号する箇所を１つのみ指定可能な実施例

図１２（ａ）は業務プログラム３－１～３－ｍから部分的暗号化装置５に入力される情報フレームのフォーマット例を示す図である。この例の情報フレームは、暗号化制御情報部５００と、複数のユーザデータから構成されるデータ部６００とから構成されている。暗号化制御情報部５００は、データ部６００に格納された一連のユーザデータのうち暗号化対象となるデータの開始位置５０１及びそのバイト数５０２を指定した１つの暗号化箇所指定情報５０３から構成される。開始位置５０１，バイト数５０２のサイズは固定長である。図１２（ｂ）に、開始位置５０１及びバイト数５０２とユーザデータとの関連を示す。開始位置５０１としては、例えば情報フレームの先頭の１バイト（つまり開始位置５０１の先頭バイト）目を０バイト目とした場合の、当該ユーザデータまでのバイト数で表現される。なお、本実施例では、部分的復号化装置６から業務プログラム３－１～３－ｍに入力される情報フレームも図１２（ａ）の形式としている。

【００４４】他方、図１２（ｃ）は部分的暗号化装置５からデータ送受信装置４に入力される情報フレームのフォーマット例を示す図である。この例の情報フレームは、復号化制御情報部７００と、複数のユーザデータから構成されるデータ部８００とから構成されている。復号化制御情報部７００は、データ部８００に格納された一連のユーザデータのうち復号化対象となるデータの開始位置７０１及びそのバイト数７０２を指定した１つの復号化箇所指定情報７０３から構成される。開始位置７０１，バイト数７０２のサイズは固定長である。開始位置７０１としては、例えば情報フレームの先頭の１バイト（つまり開始位置７０１の先頭バイト）目を０バイト目とした場合の、当該ユーザデータまでのバイト数で表現される。なお、本実施例では、データ送受信装置４から部分的復号化装置６に入力される情報フレームも図１２（ｃ）の形式としている。

【００４５】（Ａ）暗号化によりデータサイズが拡大する場合

【００４６】（ア）暗号化

この場合の部分的暗号化装置５の処理の一例を図１３のフローチャートに示す。何れかの業務プログラム３－１～３－ｍから図１２（ａ）に示したような形式の情報フレームが送られると、入力手段５１がそれを入力し（ステップＳ４１）、暗号化制御手段５２に伝達する。暗号化制御手段５２は、情報フレームの暗号化制御情報部５００を解析し（ステップＳ４２）、解析結果を制御テーブルに設定する（ステップＳ４３）。

【００４７】例えば、図１４（ａ）に示すように、各々３２バイト，３２バイト，１６バイト，１６バイト，１６バイトである５つのユーザデータＵ１，Ｕ２，Ｕ３，

Ｕ４，Ｕ５を含むデータ部６００と、ユーザデータＵ３を暗号化対象として指定した暗号化制御情報部５００とから構成される情報フレームの場合、個数，開始位置のサイズを例えば１バイト固定とすると、情報フレームの先頭から６６～８２バイト目のユーザデータＵ３が暗号化対象データであり、ユーザデータＵ３の前後のデータ（ユーザデータＵ１，Ｕ２，Ｕ４，Ｕ５）は暗号化対象データでないので、例えば図１５に示すような３つのエントリＥ１，Ｅ２，Ｅ３を持つ制御テーブル９０２を生成し、開始位置，バイト数，暗号化の有無の欄にそれぞれ図示する値を設定する。なお、この時点では、暗号化後のバイト数の欄はＮＵＬＬである。

【００４８】次に暗号化制御手段５２は、制御テーブル９０２の暗号化の有無の欄が「有」になっているエントリＥ２について、該当する箇所のデータをデータ部６００から取り出し、暗号手段５３に与えることにより暗号化する（ステップＳ４４）。

【００４９】次に暗号化制御手段５２は、暗号化後のデータサイズを図１５に示すように、エントリＥ２の暗号化後のバイト数の欄に設定する（ステップＳ４５）。

【００５０】次に暗号化制御手段５２は、図１５の制御テーブル９０２の暗号化の有無の欄が「有」になっているエントリＥ２の開始位置「６６」と暗号化後のバイト数「２４」との組を復号化箇所指定情報７０３とした復号化制御情報部７００を生成する（ステップＳ４６）。これにより、図１４（ｂ）に示す復号化制御情報部７００が生成される。

【００５１】次に暗号化制御手段５２は、図１５の制御テーブル９０２のエントリＥ１から順にエントリＥ３まで、そのエントリの暗号化の有無の欄が「有」であれば暗号化後のデータを、「無」であれば、制御テーブル９０２の開始位置の欄とバイト数の欄とで特定される入力情報フレーム上の元のデータを、データ部の先頭から順に詰め込んで、データ部８００を生成する（ステップＳ４７）。これにより、図１４（ｂ）に示すデータ部８００が生成される。

【００５２】以上のようにして復号化制御情報部７００とデータ部８００とから構成される情報フレームが生成されると、出力手段５４が、送り先および送り元の情報と共に情報フレームをデータ送受信装置４に送る（ステップＳ４８）。

【００５３】（イ）復号化

この場合の部分的復号化装置６の処理の一例を図１６のフローチャートに示す。データ送受信装置４から図１２（ｃ）に示したような形式の情報フレームが送られると、入力手段６１がそれを入力し（ステップＳ５１）、復号化制御手段６２に伝達する。復号化制御手段６２は、情報フレームの復号化制御情報部７００を解析し（ステップＳ５２）、解析結果を制御テーブルに設定する（ステップＳ５３）。

【００５４】例えば、入力された情報フレームが図１４（ｂ）に示した情報フレームであった場合、情報フレームの先頭から６６～９０バイト目のユーザデータＵ３’が復号化対象データであり、ユーザデータＵ３’の前後のデータ（ユーザデータＵ１，Ｕ２，Ｕ４，Ｕ５）は復号化対象データでないので、例えば図１７に示すような３つのエントリＥ１，Ｅ２，Ｅ３を持つ制御テーブル９０３を生成し、開始位置，バイト数，復号化の有無の欄にそれぞれ図示する値を設定する。なお、この時点では、復号化後のバイト数の欄はＮＵＬＬである。

【００５５】次に復号化制御手段６２は、制御テーブル９０３の復号化の有無の欄が「有」になっているエントリＥ２について、該当する箇所のデータをデータ部８００から取り出し、復号手段６３に与えることにより復号化する（ステップＳ５４）。

【００５６】次に復号化制御手段６２は、復号化後のデータサイズを図１５に示すように、エントリＥ２の復号化後のバイト数の欄に設定する（ステップＳ５５）。

【００５７】次に復号化制御手段６２は、図１７の制御テーブル９０３の復号化の有無の欄が「有」になっているエントリＥ２の開始位置「６６」と復号化後のバイト数「１６」との組を暗号化箇所指定情報５０３とした暗号化制御情報部５００を生成する（ステップＳ５６）。これにより、図１４（ａ）に示す暗号化制御情報部５００が生成される。

【００５８】次に復号化制御手段６２は、図１７の制御テーブル９０３のエントリＥ１から順にエントリＥ３まで、そのエントリの復号化の有無の欄が「有」であれば復号化後のデータを、「無」であれば、制御テーブル９０３の開始位置の欄とバイト数の欄とで特定される入力情報フレーム上の元のデータを、データ部の先頭から順に詰め込んで、データ部６００を生成する（ステップＳ５７）。これにより、図１４（ａ）に示すデータ部６００が生成される。

【００５９】以上のようにして暗号化制御情報部５００とデータ部６００とから構成される情報フレームが生成されると、出力手段６４が、送り元の情報と共に送り先の業務プログラムに送る（ステップＳ５８）。

【００６０】（Ｂ）暗号化によりデータサイズが拡大しない場合

【００６１】（ア）暗号化

この場合の部分的暗号化装置５の処理の一例を図１８のフローチャートに示す。何れかの業務プログラム３－１～３－ｍから図１４（ａ）に示したような形式の情報フレームが送られると、入力手段５１がそれを入力し（ステップＳ６１）、暗号化制御手段５２に伝達する。暗号化制御手段５２は、情報フレームの暗号化制御情報部５００を解析し、その開始位置５０１とバイト数５０２とで特定される箇所のデータを、データ部６００から取り出し（ステップＳ６２）、暗号手段５３に与えることに

13

より暗号化する（ステップＳ６３）。次に、生成された暗号データで、データ部６００の元の箇所を上書きする（ステップＳ６４）。そして、データ部６００が上書きされた情報フレームを、出力手段５４により、送り先および送り元の情報と共にデータ送受信装置４に送出する（Ｓ６５）。

【００６２】このように暗号化によってデータサイズが拡大せず同一サイズとなる場合、入力された情報フレームの暗号化制御情報部５００の内容は実質的に変更されず、そのまま復号化制御情報部７００となる。

【００６３】（イ）復号化

この場合の部分的復号化装置６の処理の一例を図１９のフローチャートに示す。データ送受信装置４から図１２（ｃ）に示したような形式の情報フレームが送られると、入力手段６１がそれを入力し（ステップＳ７１）、復号化制御手段６２に伝達する。復号化制御手段６２は、情報フレームの復号化制御情報部７００を解析し、その開始位置７０１及びバイト数７０２で特定される箇所のデータを、データ部８００から取り出し（ステップＳ７２）、復号手段６３に与えることにより復号化する（ステップＳ７３）。次に、生成された復号データで、データ部８００の元の箇所を上書きする（ステップＳ７４）。そして、データ部８００が上書きされた情報フレームを、出力手段６４により、送り元の情報と共に送り先の業務プログラムに送出する（Ｓ７５）。

【００６４】このように復号化によってデータサイズが拡大せず同一サイズとなる場合、入力された情報フレームの復号化制御情報部７００の内容は実質的に変更されず、そのまま暗号化制御情報部５００となる。

【００６５】以上の実施の形態は、情報処理装置間で送受信されるデータに対する暗号化，復号化に本発明を適用したが、情報処理装置上の業務プログラムがデータを暗号化してローカルな記憶装置に記録する場合の記録データの暗号化、記録されたデータの復号化にも本発明は適用可能である。

【００６６】

【発明の効果】以上説明したように本発明によれば以下のような効果が得られる。

【００６７】一連のデータ中の暗号化したい箇所をよりきめ細かく指定することができる。その理由は、一連のデータのうち暗号化したいデータの開始位置だけでなく、その長さも指定することができるからであり、また、開始位置と長さを複数組指定することができるからである。

【００６８】このように暗号化したい箇所をきめ細かく指定できるため、必要最小限の暗号化が可能となり、暗号化処理時間の大幅な短縮が可能となる。

【図面の簡単な説明】

【図１】本発明を適用した情報処理装置の一例を示すブロック図である。

14

【図２】部分的暗号化装置の構成例を示すブロック図である。

【図３】部分的復号化装置の構成例を示すブロック図である。

【図４】情報フレームのフォーマットの一例を示す図である。

【図５】部分的暗号化装置の処理例を示すフローチャートである。

【図６】情報フレームの具体例を示す図である。

【図７】部分的暗号化装置が使用する制御テーブルの例を示す図である。

【図８】部分的復号化装置の処理例を示すフローチャートである。

【図９】部分的復号化装置が使用する制御テーブルの例を示す図である。

【図１０】部分的暗号化装置の処理例を示すフローチャートである。

【図１１】部分的復号化装置の処理例を示すフローチャートである。

【図１２】情報フレームのフォーマット例を示す図である。

【図１３】部分的暗号化装置の処理例を示すフローチャートである。

【図１４】情報フレームの具体例を示す図である。

【図１５】部分的暗号化装置が使用する制御テーブルの例を示す図である。

【図１６】部分的復号化装置の処理例を示すフローチャートである。

【図１７】部分的復号化装置が使用する制御テーブルの例を示す図である。

【図１８】部分的暗号化装置の処理例を示すフローチャートである。

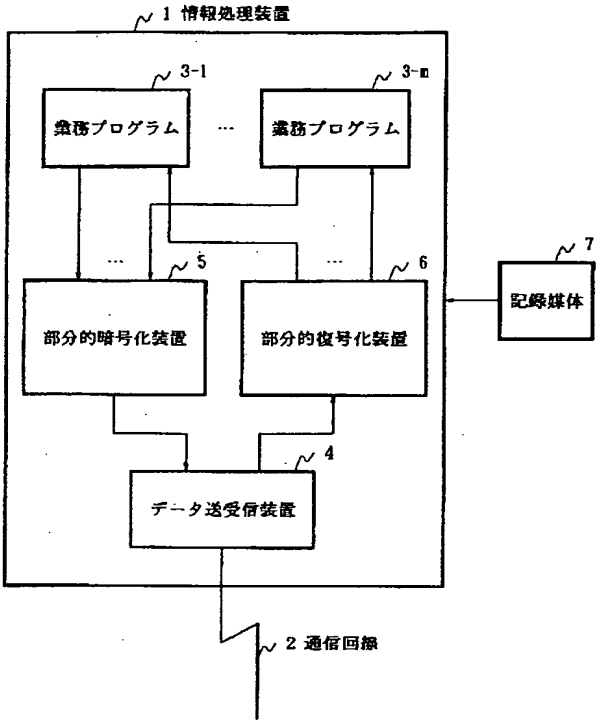
【図１９】部分的復号化装置の処理例を示すフローチャートである。

【図２０】従来の問題点の説明図である。

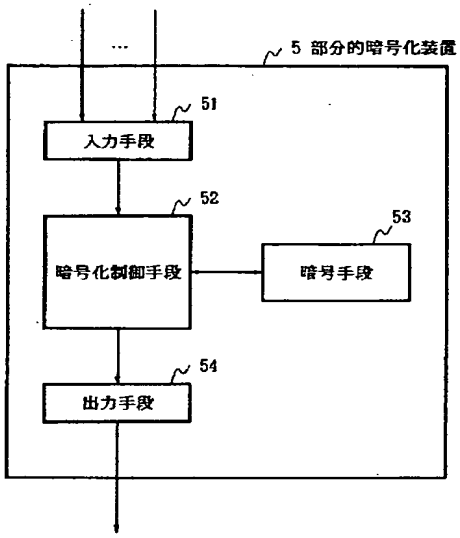
【符号の説明】

１…情報処理装置
２…通信回線
３－１～３－ｍ…業務プログラム
４…データ送受信装置
５…部分的暗号化装置
６…部分的復号化装置
７…記録媒体
５１，６１…入力手段
５２…暗号化制御手段
５３…暗号手段
５４，６４…出力手段
６２…復号化制御手段
６３…復号手段

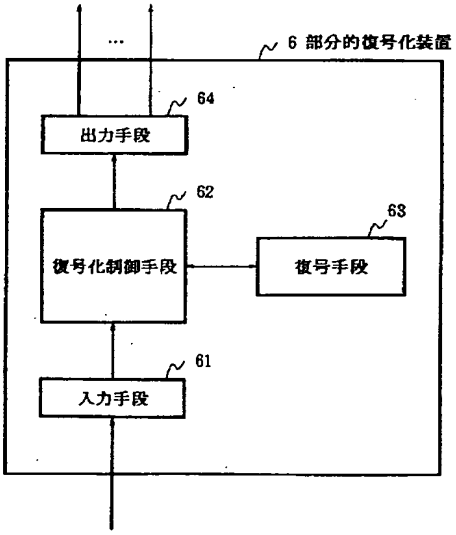
【図１】


1 情報処理装置
3-1
3-n
業務プログラム
…
業務プログラム
…
5
6
7
部分的暗号化装置
部分的復号化装置
記録媒体
4
データ送受信装置
2 通信回線

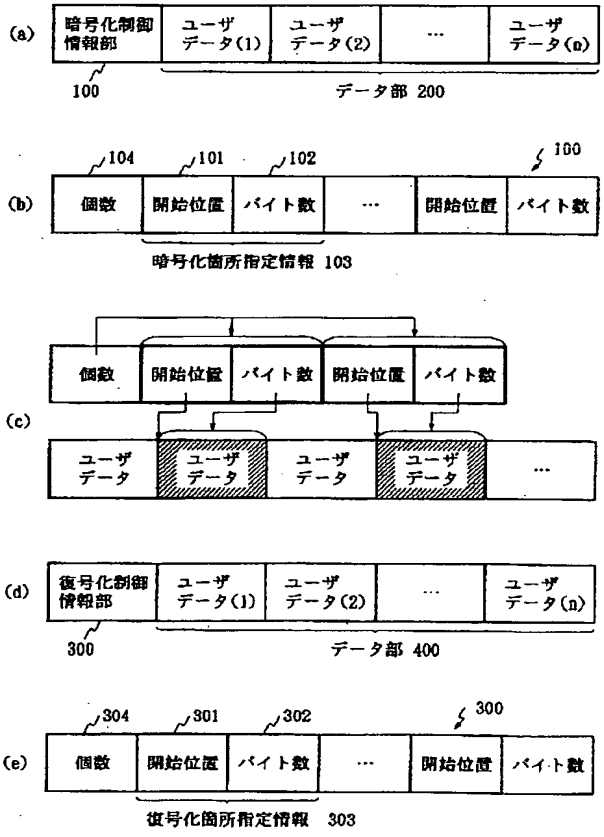
【図２】


…
5 部分的暗号化装置
51
入力手段
52
53
暗号化制御手段
暗号手段
54
出力手段

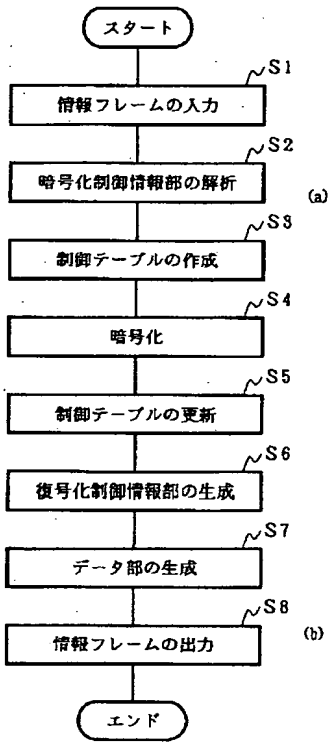
【図３】


…
6 部分的復号化装置
64
出力手段
62
63
復号化制御手段
復号手段
61
入力手段

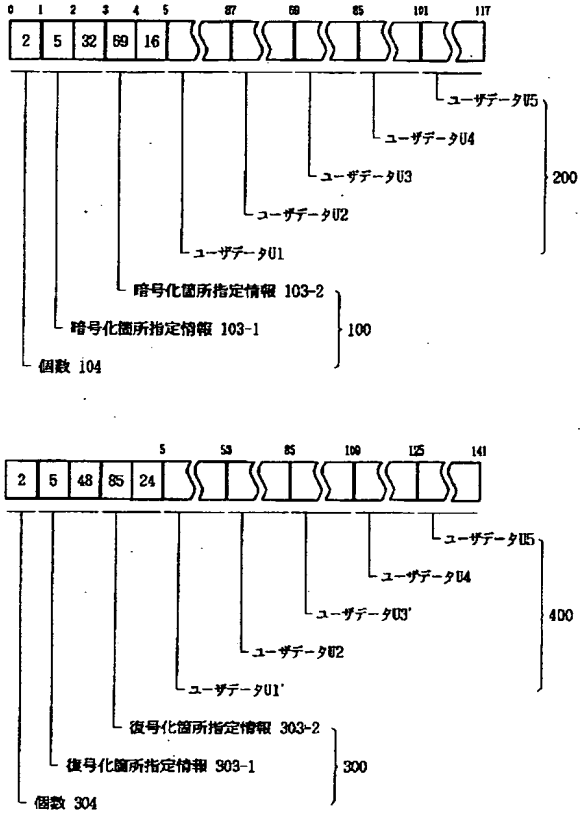
【図４】


(a)
暗号化制御情報部
ユーザデータ(1)
ユーザデータ(2)
…
ユーザデータ(n)
100
データ部 200
(b)
104
101
102
100
個数
開始位置
バイト数
…
開始位置
バイト数
暗号化箇所指定情報 103
(c)
個数
開始位置
バイト数
開始位置
バイト数
ユーザデータ
ユーザデータ
ユーザデータ
ユーザデータ
…
(d)
復号化制御情報部
ユーザデータ(1)
ユーザデータ(2)
…
ユーザデータ(n)
300
データ部 400
(e)
304
301
302
300
個数
開始位置
バイト数
…
開始位置
バイト数
復号化箇所指定情報 303

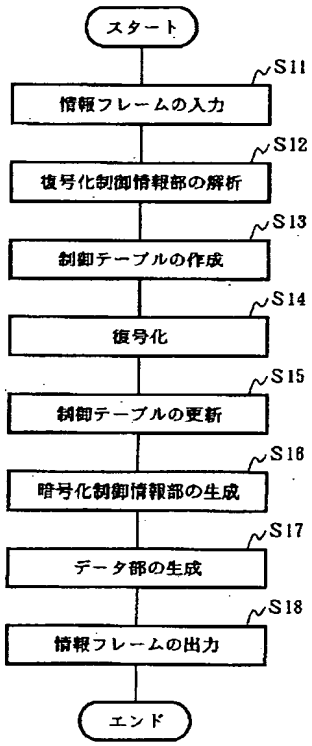
【図５】



【図６】



【図８】



【図７】

900

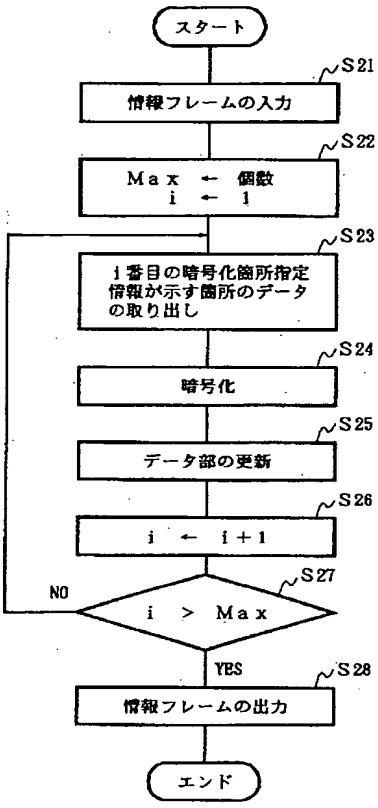
開始位置	バイト数	暗号化の有無	暗号化後の開始位置	暗号化後のバイト数	
5	32	有	5	48	E1
37	32	無	53	－	E2
69	16	有	85	24	E3
85	32	無	109	－	E4

【図９】

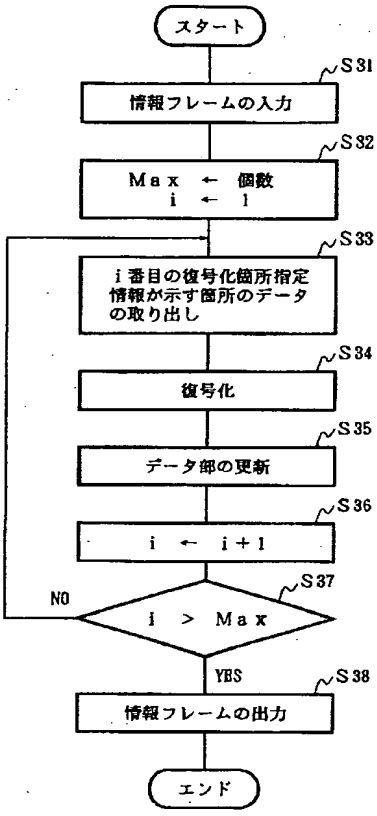
901

開始位置	バイト数	復号化の有無	復号化後の開始位置	復号化後のバイト数	
5	48	有	5	32	E1
53	32	無	37	－	E2
85	24	有	69	16	E3
109	32	無	85	－	E4

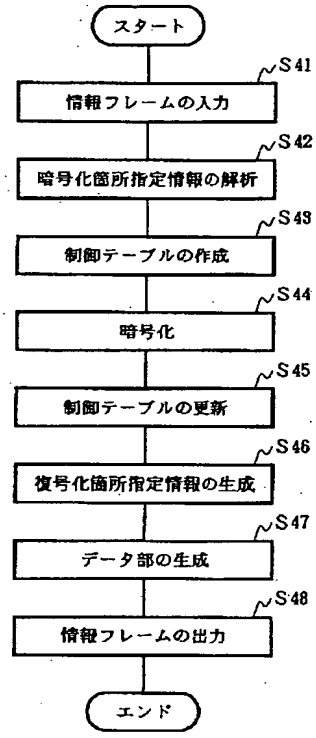
【図１０】



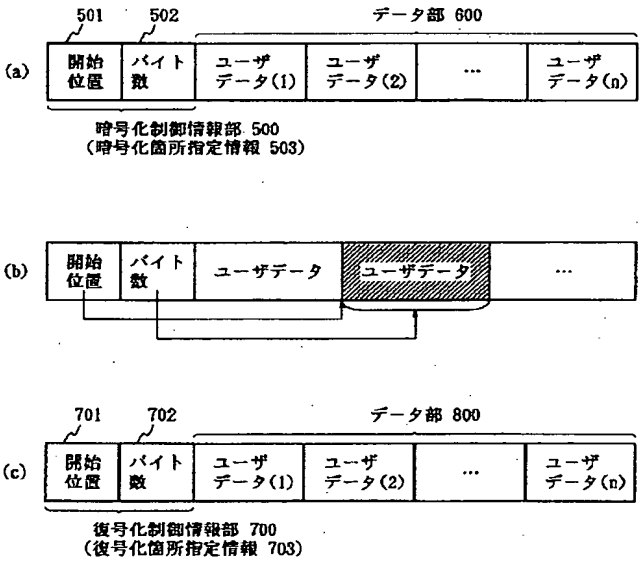
【図１１】



【図１３】



【図１２】

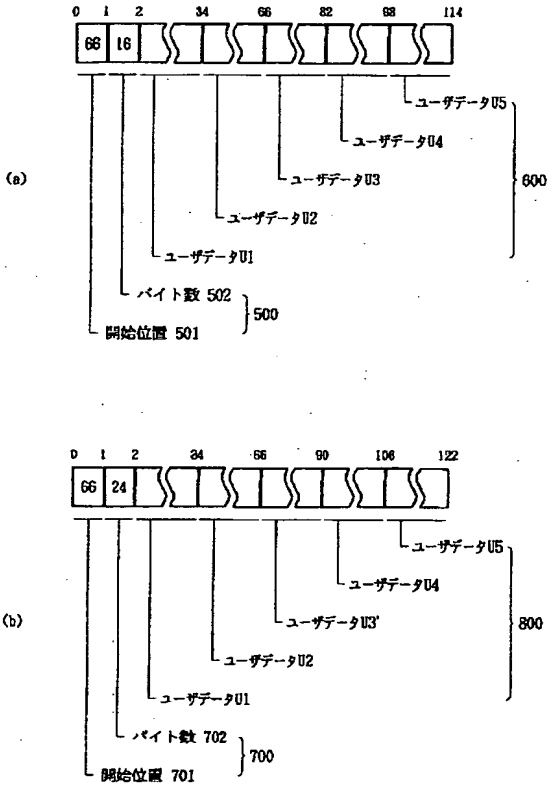


【図１５】

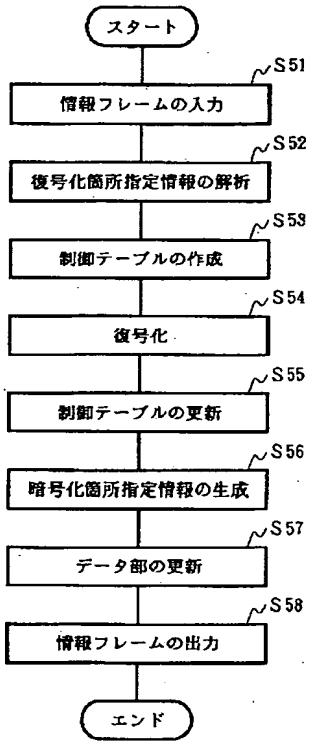
902

開始位置	バイト数	暗号化の有無	暗号化後のバイト数	
2	64	無	－	B1
66	16	有	24	B2
82	32	無	－	B3

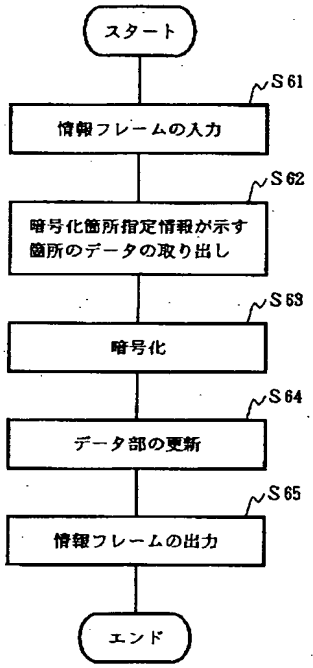
【図１４】



【図１６】



【図１８】

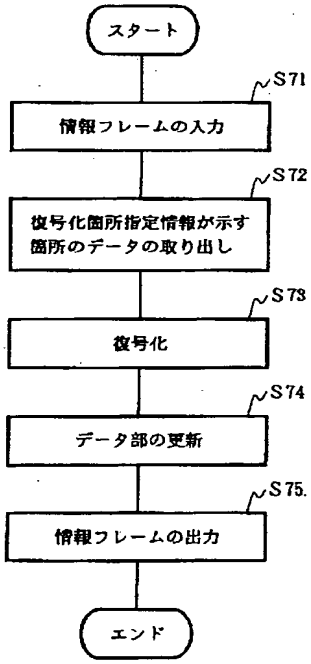


【図１７】

903

開始位置	バイト数	復号化の有無	復号化後のバイト数	
2	64	無	－	E1
66	24	有	16	E2
90	32	無	－	E3

【図１９】



【図２０】